

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): WINEGARD, Robert

Examiner: WOO, Stella L.

Serial No.: 10/663,036

Group Art Unit: 2614

Filed: September 15, 2003

Docket: 1222-2

Dated: February 17, 2009

For: **INTEGRATED SECURE ENCRYPTION APPARATUS**

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

TRANSMITTAL OF APPELLANTS' BRIEF ON APPEAL

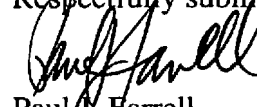
Sir:

Enclosed please find APPELLANTS' BRIEF.

Also enclosed is a credit card payment in the amount of \$540.00 to cover the appeal fee.

If the enclosed credit card payment is insufficient for any reason or becomes detached, please charge the required fee under 37 C.F.R. §1.17 to Deposit Account No. 50-4053. Also, in the event any additional extensions of time are required, please treat this paper as a petition to extend the time as required and charge Deposit Account No. 50-4053.

Respectfully submitted,



Paul V. Farrell

Reg. No.: 33,494

Attorney for Applicant(s)

THE FARRELL LAW FIRM
333 Earle Ovington Blvd., Suite 701
Uniondale, New York 11553
516-228-3565

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
BOARD OF PATENT APPEALS AND INTERFERENCES**

APPLICANT(S): WINEGARD, Robert

GROUP ART UNIT: 2614

APPLICATION NO.: 10/663,036

EXAMINER: WOO, Stella L.

FILING DATE: September 15, 2003

DOCKET: 1222-2

DATED: February 17, 2009

FOR: INTEGRATED SECURE ENCRYPTION APPARATUS

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF ON APPEAL

REAL PARTY IN INTEREST

The real party in interest is Criticom, Inc., the assignee of the subject application, having an office at 4211 Forbes Boulevard, Lanham, Maryland, 20706, United States of America.

RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge and belief, there are no currently pending related appeals, interferences or judicial proceedings.

STATUS OF CLAIMS

Original Claims 1-25 were filed on September 15, 2003. Claims 1, 19 and 25 were amended in an Amendment filed April 9, 2008. Thus, Claims 1-25 are pending in the Appeal. Claims 1, 19 and 25 are in independent form. For the purposes of this Appeal, Claims 1-18 stand or fall together, Claims 19-24 stand or fall together, and Claim 25 stands or falls alone.

STATUS OF AMENDMENTS

Thus, the Appendix to this Appeal Brief includes Claims 1, 19 and 25, of which the status is indicated as “Previously Presented”; and Claims 2-18 and 20-24, of which the status is indicated as “Original”.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention as recited in Claim 1 relates to an integrated secure videoconferencing communications system. The integrated secure videoconferencing communications system includes an inverse multiplexer for receiving and converting data. (Specification at page 6, lines 14-21, FIG. 1.)¹ The integrated secure videoconferencing communications system further includes a black side switch having a first relay that includes a first contact, a second contact, and a third contact, and coupled to the inverse multiplexer via the third contact. (Specification at page 6, lines 19-21, FIG. 1.) The integrated secure videoconferencing communications system still further includes an encryption device coupled to the second contact of the black side switch. (Specification at page 6, lines 23-25, FIG. 1.) The integrated secure videoconferencing communications system yet further includes a red side switch having a second relay that includes a first contact, a second contact, and a third contact, and coupled to the encryption device via the second contact. (Specification at page 6, lines 19-25, FIG. 1.) The integrated secure videoconferencing communications system still yet further includes a codec coupled to the red side switch via the third contact of the red side switch. (Specification at page 6, lines 26-27, FIG. 1.) The integrated secure videoconferencing communications system also includes a controller coupled to the black side and the red side switches for powering down the switches in a secure mode and powering up the switches in a non-secure mode, wherein in the secure mode the relays default to connect the encryption device into a communication path. (Specification at page 9, lines 6-9, FIG. 1.)

The invention as recited in Claim 19 relates to a method for providing secure communications. The method for providing secure communications includes determining an

operating mode. (Specification at page 9, lines 6-9, FIGs. 3A and 3B.) The method for providing secure communications further includes if the operating mode is secure mode, powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module. (Specification at page 9, lines 10-20, FIGs. 3A and 3B.) The method for providing secure communications also includes if the operating mode is non-secure mode, powering up and enabling first contacts of the two switches and communicating data between the two switches directly. (Specification at page 9, lines 21-31, FIGs. 3A and 3B.)

The invention as recited in Claim 25 relates to an integrated secure videoconferencing communications system. The integrated secure videoconferencing communications system includes an inverse multiplexer for receiving and converting data. (Specification at page 6, lines 14-21, FIG. 1.) The integrated secure videoconferencing communications system further includes a black side switch connected to the inverse multiplexer. (Specification at page 6, lines 19-21, FIG. 1.) The integrated secure videoconferencing communications system still further includes an encryption device connected to the black side switch. (Specification at page 6, lines 23-25, FIG. 1.) The integrated secure videoconferencing communications system yet further includes a red side switch connected to the encryption device, and connected to the black side switch. (Specification at page 6, lines 19-25, FIG. 1.) The integrated secure videoconferencing communications system still yet further includes a codec connected to the red side switch. (Specification at page 6, lines 26-27, FIG. 1.) The integrated secure videoconferencing communications system also includes a controller for controlling the black side and the red side switches to power down and default to a secure path connection between the black side and the red side switches via the encryption device or to power up

¹ Although a citation for each feature of the claims is provided herein, Appellant does not concede

and enable a non secure path connection directly between the black side and the red side switches.

(Specification at page 9, lines 10-31, FIG. 1.)

the fact that support may be found elsewhere in the written description.

GROUND FOR REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 1-25 under 35 U.S.C. §103(a) are rendered obvious over U.S. Patent 6,549,229 (Kirby) in view of U.S. Patent 4,903,298 (Cline).

ARGUMENT

1. The Examiner has failed to make out a prima facie case for an obviousness rejection under 35 U.S.C. §103(a) of Claims 2-25

The Examiner has failed to make a prima facie case for a §103(a) rejection regarding the recitations of Claims 2-25, as the Examiner has failed to address and has failed to properly cite any sections of Kirby or Cline that teach the recitations of the claims.² In the final Office Action, the Examiner only addresses the recitations of Claim 1. The final Office Action is silent as to any of the features of Claims 2-25.

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. §103(a).

Section 2143.03 of the MPEP requires the “consideration” of every claim feature in an obviousness determination. To render a claim unpatentable, however, the Office must do more than merely “consider” each and every feature for this claim. Instead, the asserted combination must also teach or suggest *each and every claim feature*. See *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974) (emphasis added) (to establish *prima facie* obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art). Indeed, as the Board of Patent Appeal and Interferences has recently confirmed, a proper obviousness determination requires that an Examiner make “a searching comparison of the claimed invention – *including all its limitations* – with the teaching of the prior art.” See *In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis in original). Further, the necessary presence of all claim features is axiomatic, since the Supreme Court has long held that obviousness is a

² See final Office Action dated July 17, 2008 at pages 2-3.

question of law based on underlying factual inquiries, including ... ascertaining the differences between *the claimed invention* and the prior art. *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966) (emphasis added). Indeed, Applicant submits that this is why Section 904 of the MPEP instructs Examiners to conduct an art search that covers “the invention *as described and claimed*.” (emphasis added). Lastly, Applicant respectfully directs attention to MPEP § 2143, the instructions of which buttress the conclusion that obviousness requires at least a suggestion of all of the features of a claim, since the Supreme Court in *KSR Int’l v. Teleflex Inc.* stated that “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR Int’l v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007) (*quoting In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

In sum, it remains well-settled law that obviousness requires at least a suggestion of all of the features in a claim. *See In re Wada and Murphy, citing CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) and *In re Royka*, 490 F.2d 981, 985.

Thus, since the Examiner has not addressed any of the features of Claims 2-25, the rejection of Claims 2-25 must be reversed.

2. Independent Claim 1 is patentable over Kirby in view of Cline

Independent Claim 1 was said to be rendered obvious by Kirby in view of Cline.³

The invention as recited in Claim 1 relates to an integrated secure videoconferencing communications system. The integrated secure videoconferencing communications system includes an inverse multiplexer for receiving and converting data. The integrated secure videoconferencing

³ See Office Action dated July 17, 2008 at pages 2-3.

communications system further includes a black side switch having a first relay that includes a first contact, a second contact, and a third contact, and coupled to the inverse multiplexer via the third contact. The integrated secure videoconferencing communications system still further includes an encryption device coupled to the second contact of the black side switch. The integrated secure videoconferencing communications system yet further includes a red side switch having a second relay that includes a first contact, a second contact, and a third contact, and coupled to the encryption device via the second contact. The integrated secure videoconferencing communications system still yet further includes a codec coupled to the red side switch via the third contact of the red side switch. The integrated secure videoconferencing communications system also includes a controller coupled to the black side and the red side switches for powering down the switches in a secure mode and powering up the switches in a non-secure mode, wherein in the secure mode the relays default to connect the encryption device into a communication path.

Kirby discloses a small, portable, self-contained, video teleconferencing system.⁴

Cline discloses a system for providing encryption and decryption of voice and data transmissions to and from an aircraft.⁵

2A. The combination of Kirby and Cline does not teach or disclose at least powering down the switches in a secure mode, as recited in Claim 1, and therefore Kirby in view of Cline cannot render Claim 1 unpatentable

Claim 1 of the present application recites, in part, a controller coupled to the black side and the red side switches for powering down the switches in a secure mode and powering up the

⁴ See Kirby at title and abstract.

switches in a non-secure mode, wherein in the secure mode (i.e. power down mode) the relays default to connect the encryption device into a communication path. One of the central concepts of the present invention is to provide secure communications during a power down state. The power down state can be intentional (turning off the power switch) or unintentional (loss of power supplied from the power grid). In either case, when power is not supplied to the device of Claim 1, the device will ensure that the communication path is in a secure mode.

The Examiner relies on Cline as disclosing these features of Claim 1.⁶

In FIG. 6, Cline illustrates what is referred to as its clear mode or unenergized state.⁷ In this state no power is supplied to the device disclosed by Cline. Cline states in col. 14, lines 20-30:

Referring now to FIG. 6 in particular, the transmission paths for the encryption/decryption unit 200 are illustrated for the condition when the active control unit is in the clear mode. All the relays 210-218 are shown in their unenergized states with an electrical connection through the normally closed contacts of each relay and no electrical connection through the normally open contacts. That is, the connections shown in FIG. 6 are those that occur when no power is applied to the coils of the relays.

As shown in FIG. 6, relays 210A, 212A and 214A route signals directly from the aircraft audio routing system 136 to the transceivers 130, 132 and 134. In the unenergized state shown in FIG. 6, none of the signals are routed through the encryption module 202A. Cline unambiguously teaches a system that defaults to an unencrypted mode when no power is supplied to its device.

Cline fails to teach or suggest powering down the switches in a secure mode, as recited in Claim 1 of the present application. Kirby does not cure the defects of Cline.

⁵ See Cline at title and abstract.

⁶ See final Office Action dated July 17, 2008 at pages 2-3.

⁷ See Cline at col. 14, lines 20-24.

Based on at least the foregoing, Claim 1 is patentable over the combination of Kirby in view of Cline, and therefore the rejection of independent Claim 1 under §103(a) must be reversed.

2B. The combination of Kirby and Cline teaches away from powering down the switches in a secure mode, as recited in Claim 1, and therefore Kirby in view of Cline cannot render Claim 1 unpatentable

“When the prior art teaches away from combining certain known elements, discovery of successful means of combining them is more likely to be nonobvious.” *KSR*, 550 U.S. at 398, 82 USPQ2d at 1395.

Claim 1 of the present application recites powering down the switches in a secure mode. Thus, when no power is supplied to the apparatus of Claim 1, the apparatus defaults to a secure mode.

Cline teaches that its clear mode (i.e. non-encrypted mode) is the preferred mode. At col. 14, lines 30-34, Cline states, “Since the clear mode is likely to be the most frequently occurring mode, this is a particularly advantageous feature because the circuit does not require the power to energize a coil to maintain this mode.”

Cline teaches away from the present invention.

Based on at least the foregoing, Claim 1 is patentable over the combination of Kirby in view of Cline, and therefore the rejection of independent Claim 1 under §103(a) must be reversed.

2C. Independent Claim 1 is not rendered obvious by Kirby in view of Cline

The Examiner has failed to show that each and every element of Claim 1, and in as complete

detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 1 is allowable.

3. Dependent Claims 2-18 are patentable over Kirby in view of Cline

Without conceding the patentability per se of dependent Claims 2-18, these claims are likewise believed to be allowable by virtue of at least their dependence on Claim 1.

4. Independent Claim 19 is patentable over Kirby in view of Cline

Independent Claim 19 was said to be rendered obvious by Kirby in view of Cline.⁸

The invention as recited in Claim 19 relates to a method for providing secure communications. The method for providing secure communications includes determining an operating mode. The method for providing secure communications further includes if the operating mode is secure mode, powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module. The method for providing secure communications also includes if the operating mode is non-secure mode, powering up and enabling first contacts of the two switches and communicating data between the two switches directly.

Kirby discloses a small, portable, self-contained, video teleconferencing system.⁹

Cline discloses a system for providing encryption and decryption of voice and data transmissions to and from an aircraft.¹⁰

⁸ See Office Action dated July 17, 2008 at pages 2-3.

⁹ See Kirby at title and abstract.

¹⁰ See Cline at title and abstract.

4A. The combination of Kirby and Cline does not teach or disclose at least powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module, as recited in Claim 19, and therefore Kirby in view of Cline cannot render Claim 19 unpatentable

Claim 19 recites, in part, if the operating mode is the secure mode, **powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module**; and if the operating mode is the non-secure mode, powering up and enabling first contacts of the two switches and communicating data between the two switches directly. One of the central concepts of the present invention is to provide secure communications during a power down state. The power down state can be intentional (turning off the power switch) or unintentional (loss of power supplied from the power grid). In either case, when power is not supplied to the device of Claim 19, the device will ensure that the communication path is in a secure mode.

It is presumed¹¹ that the Examiner would rely on Cline as disclosing these features.¹²

In FIG. 6, Cline illustrates what is referred to as its clear mode or unenergized state.¹³ In this state no power is supplied to the device disclosed by Cline. Cline states in col. 14, lines 20-30:

Referring now to FIG. 6 in particular, the transmission paths for the encryption/decryption unit 200 are illustrated for the condition when the active control unit is in the clear mode. All the relays 210-218 are shown in their unenergized states with an electrical connection through the normally closed contacts of each relay and no electrical connection through the normally open contacts. That is, the connections shown in FIG. 6 are those that occur when no power is applied to the coils of the relays.

¹¹ See Section 1, *supra*.

¹² See final Office Action dated July 17, 2008 at pages 2-3.

¹³ See Cline at col. 14, lines 20-24.

As shown in FIG. 6, relays 210A, 212A and 214A route signals directly from the aircraft audio routing system 136 to the transceivers 130, 132 and 134. In the unenergized state shown in FIG. 6, none of the signals are routed through the encryption module 202A. Cline unambiguously teaches a system that defaults to an unencrypted mode when no power is supplied to its device.

Cline fails to teach or suggest powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module, as recited in Claim 19 of the present application. Kirby does not cure the defects of Cline.

Based on at least the foregoing, Claim 19 is patentable over the combination of Kirby in view of Cline, and therefore the rejection of independent Claim 19 under §103(a) must be reversed.

4B. The combination of Kirby and Cline teaches away from powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module, as recited in Claim 19, and therefore Kirby in view of Cline cannot render Claim 19 unpatentable

“When the prior art teaches away from combining certain known elements, discovery of successful means of combining them is more likely to be nonobvious.” *KSR*, 550 U.S. at 398, 82 USPQ2d at 1395.

Claim 19 of the present application recites powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module. Thus, when no power is supplied to the apparatus of Claim 19, the apparatus defaults to a secure mode.

Cline teaches that its clear mode (i.e. non-encrypted mode) is the preferred mode. At col. 14, lines 30-34, Cline states, “Since the clear mode is likely to be the most frequently occurring mode, this is a particularly advantageous feature because the circuit does not require the power to energize a

coil to maintain this mode.”

Cline teaches away from the present invention.

Based on at least the foregoing, Claim 19 is patentable over the combination of Kirby in view of Cline, and therefore the rejection of independent Claim 19 under §103(a) must be reversed.

4C. Independent Claim 19 is not rendered obvious by Kirby in view of Cline

The Examiner has failed to show that each and every element of Claim 19, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 19 is allowable.

5. Dependent Claims 20-24 are patentable over Kirby in view of Cline

Without conceding the patentability per se of dependent Claims 20-24, these claims are likewise believed to be allowable by virtue of at least their dependence on Claim 19.

6. Independent Claim 25 is patentable over Kirby in view of Cline

Independent Claim 25 was said to be rendered obvious by Kirby in view of Cline.¹⁴

The invention as recited in Claim 25 relates to an integrated secure videoconferencing communications system. The integrated secure videoconferencing communications system includes an inverse multiplexer for receiving and converting data. The integrated secure videoconferencing communications system further includes a black side switch connected to the inverse multiplexer. The integrated secure videoconferencing communications system still further includes an encryption

¹⁴ See Office Action dated July 17, 2008 at pages 2-3.

device connected to the black side switch. The integrated secure videoconferencing communications system yet further includes a red side switch connected to the encryption device, and connected to the black side switch. The integrated secure videoconferencing communications system still yet further includes a codec connected to the red side switch. The integrated secure videoconferencing communications system also includes a controller for controlling the black side and the red side switches to power down and default to a secure path connection between the black side and the red side switches via the encryption device or to power up and enable a non secure path connection directly between the black side and the red side switches.

Kirby discloses a small, portable, self-contained, video teleconferencing system.¹⁵

Cline discloses a system for providing encryption and decryption of voice and data transmissions to and from an aircraft.¹⁶

6A. The combination of Kirby and Cline does not teach or disclose at least to power down and default to a secure path, as recited in Claim 25, and therefore Kirby in view of Cline cannot render Claim 25 unpatentable

Claim 25 of the present application recites, in part, a controller for controlling the black side and the red side switches to **power down and default to a secure path** connection between the black side and the red side switches via the encryption device or to power up and enable a non-secure path connection directly between the black side and the red side switches. One of the central concepts of the present invention is to provide secure communications during a power down state. The power down state can be intentional (turning off the power switch) or unintentional (loss of power being

¹⁵ See Kirby at title and abstract.

supplied from the power grid). In either case, when power is not supplied to the device of Claim 25, the device will ensure that the communication path is in a secure mode.

It is presumed¹⁷ that the Examiner would rely on Cline as disclosing these features.¹⁸

In FIG. 6, Cline illustrates what is referred to as its clear mode or unenergized state.¹⁹ In this state no power is supplied to the device disclosed by Cline. Cline states in col. 14, lines 20-30:

Referring now to FIG. 6 in particular, the transmission paths for the encryption/decryption unit 200 are illustrated for the condition when the active control unit is in the clear mode. All the relays 210-218 are shown in their unenergized states with an electrical connection through the normally closed contacts of each relay and no electrical connection through the normally open contacts. That is, the connections shown in FIG. 6 are those that occur when no power is applied to the coils of the relays.

As shown in FIG. 6, relays 210A, 212A and 214A route signals directly from the aircraft audio routing system 136 to the transceivers 130, 132 and 134. In the unenergized state shown in FIG. 6, none of the signals are routed through the encryption module 202A. Cline unambiguously teaches a system that defaults to an unencrypted mode when no power is supplied to its device.

Cline fails to teach or suggest to power down and default to a secure path, as recited in Claim 25 of the present application. Kirby does not cure the defects of Cline.

Based on at least the foregoing, Claim 25 is patentable over the combination of Kirby in view of Cline, and therefore the rejection of independent Claim 25 under §103(a) must be reversed.

6B. The combination of Kirby and Cline teaches away from powering down the switches in a secure

¹⁶ See Cline at title and abstract.

¹⁷ See Section 1, *supra*.

¹⁸ See final Office Action dated July 17, 2008 at pages 2-3.

mode, as recited in Claim 25, and therefore Kirby in view of Cline cannot render Claim 25 unpatentable

“When the prior art teaches away from combining certain known elements, discovery of successful means of combining them is more likely to be nonobvious.” *KSR*, 550 U.S. at 398, 82 USPQ2d at 1395.

Claim 25 of the present application recites to power down and default to a secure path. Thus, when no power is supplied to the apparatus of Claim 25, the apparatus defaults to a secure mode.

Cline teaches that its clear mode (i.e. non-encrypted mode) is the preferred mode. At col. 14, lines 30-34, Cline states, “Since the clear mode is likely to be the most frequently occurring mode, this is a particularly advantageous feature because the circuit does not require the power to energize a coil to maintain this mode.”

Cline teaches away from the present invention.

Based on at least the foregoing, Claim 25 is patentable over the combination of Kirby in view of Cline, and therefore the rejection of independent Claim 25 under §103(a) must be reversed.

6C. Independent Claim 25 is not rendered obvious by Kirby in view of Cline

The Examiner has failed to show that each and every element of Claim 25, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 25 is allowable.

¹⁹ See Cline at col. 14, lines 20-24.

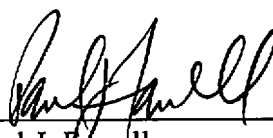
CONCLUSION

As the Examiner has failed to make out a prima facie case for an obviousness rejection, the rejection of Claims 1-25 must be reversed.

It is well settled that in order for a rejection under 35 U.S.C. §103(a) to be appropriate, the claimed invention must be shown to be obvious in view of the prior art as a whole. A claim may be found to be obvious if it is first shown that all of the recitations of a claim are taught in the prior art or are suggested by the prior art. In re Royka, 490 F.2d 981, 985, 180 U.S.P.Q. 580, 583 (C.C.P.A. 1974), cited in M.P.E.P. §2143.03. The Examiner has failed to show that all of the recitations of Claims 1-25 are taught or suggested by Kirby in view of Cline

Accordingly, the Examiner has failed to make out a prima facie case for an obviousness rejection. Independent Claims 1-25 are not rendered unpatentable by Kirby in view of Cline. Therefore, the rejections of Claims 1-25 must be reversed.

Dated: February 17, 2009

By: 
Paul J. Farrell
Reg. No.: 33,494
Attorney for Appellants

THE FARRELL LAW FIRM, P.C.
333 Earle Ovington Blvd., Suite 701
Uniondale, New York 11553
(516) 228-3565 (tel)
(516) 228-8475 (fax)

CLAIMS APPENDIX

1. (Previously Presented) An integrated secure videoconferencing communications system, comprising:

an inverse multiplexer for receiving and converting data;

a black side switch having a first relay that includes a first contact, a second contact, and a third contact, and coupled to the inverse multiplexer via the third contact;

an encryption device coupled to the second contact of the black side switch;

a red side switch having a second relay that includes a first contact, a second contact, and a third contact, and coupled to the encryption device via the second contact;

a codec coupled to the red side switch via the third contact of the red side switch; and

a controller coupled to the black side and the red side switches for powering down the switches in a secure mode and powering up the switches in a non-secure mode, wherein in the secure mode the relays default to connect the encryption device into a communication path.

2. (Original) The system of claim 1, wherein if the system is operating in a secure mode, the controller disables the first contacts of the black side and the red side switches, and the second contacts of the black side and red side switches are enabled to connect data path via the encryption device.

3. (Original) The system of claim 1, wherein if the system is operating in a non-secure mode, the controller enables the first contacts of the black and the red side switches.

4. (Original) The system of claim 1, further comprising means for on-screen dialing.
5. (Original) The system of claim 1, further comprising fiber optic isolation between all secure and non-secure signals.
6. (Original) The system of claim 1, wherein the system is in a secure operating mode when power is not supplied to the system.
7. (Original) The system of claim 1, further including:
 - a first fiber optics modem coupled to the first contact of the black side switch; and
 - a second fiber optics modem coupled to the first contact of the red side switch,wherein data is communicated between the inverse multiplexer and the codec via the first and the second fiber optics modems.
8. (Original) The system of claim 1, further including a dial isolator module coupled to the codec by a first interface, the dial isolator further coupled to the inverse multiplexer by a second interface.
9. (Original) The system of claim 1, wherein the black side switch is coupled to the inverse multiplexer via an RS-530/449 interface.
10. (Original) The system of claim 1, wherein the red side switch is coupled to the codec via

an RS-530/449 interface.

11. (Original) The system of claim 1, further including a power control module coupled to the controller and the first and the second fiber optics modems.

12. (Original) The system of claim 11, wherein the power control module terminates power supplied to the first and the second fiber optics modems when the system is operating in a secure mode.

13. (Original) The system of claim 1, further including a status indicator coupled to the controller for indicating an operating mode.

14. (Original) The system of claim 1, further including a switch coupled to the controller for selecting an operating mode.

15. (Original) The system of claim 1, wherein the encryption device is coupled to the black side and the red side switches via an RS-530/449 interface.

16. (Original) The system of claim 1, wherein the codec includes a serial interfaced videoconferencing codec.

17. (Original) The system of claim 1, wherein the encryption device includes KIV 7 module.

18. (Original) The system of claim 1, wherein the encryption device includes KIV 19 module.
19. (Previously Presented) A method for providing secure communications, comprising:
determining an operating mode;
if the operating mode is secure mode, powering down and defaulting to second contacts of two switches and communicating data between the two switches via a secure module; and
if the operating mode is non-secure mode, powering up and enabling first contacts of the two switches and communicating data between the two switches directly.
20. (Original) The method of claim 19, further including displaying the operating mode.
21. (Original) The method of claim 19, further including if the operating mode is non-secure mode, routing data between the two switches via a plurality of fiber optics modems.
22. (Original) The method of claim 19, further including if the operating mode is secure, routing data between the two switches through encryption devices and disconnecting the non-secure path between the two switches.
23. (Original) The method of claim 19, further including if the operating mode is secure, terminating power from a plurality of fiber optics modems coupling the two switches.

24. (Original) The method of claim 19, further including converting ISDN channel data to high speed RS-530/499 data.

25. (Previously Presented) An integrated secure videoconferencing communications system, comprising:

- an inverse multiplexer for receiving and converting data;

- a black side switch connected to the inverse multiplexer;

- an encryption device connected to the black side switch;

- a red side switch connected to the encryption device, and connected to the black side switch;

- a codec connected to the red side switch; and

- a controller for controlling the black side and the red side switches to power down and default to a secure path connection between the black side and the red side switches via the encryption device or to power up and enable a non secure path connection directly between the black side and the red side switches.

EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. 1.130, 1.131, 1.132 or entered by the Examiner and relied upon by Appellant.

RELATED PROCEEDINGS APPENDIX

There are no known decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 C.F.R. 41.37.